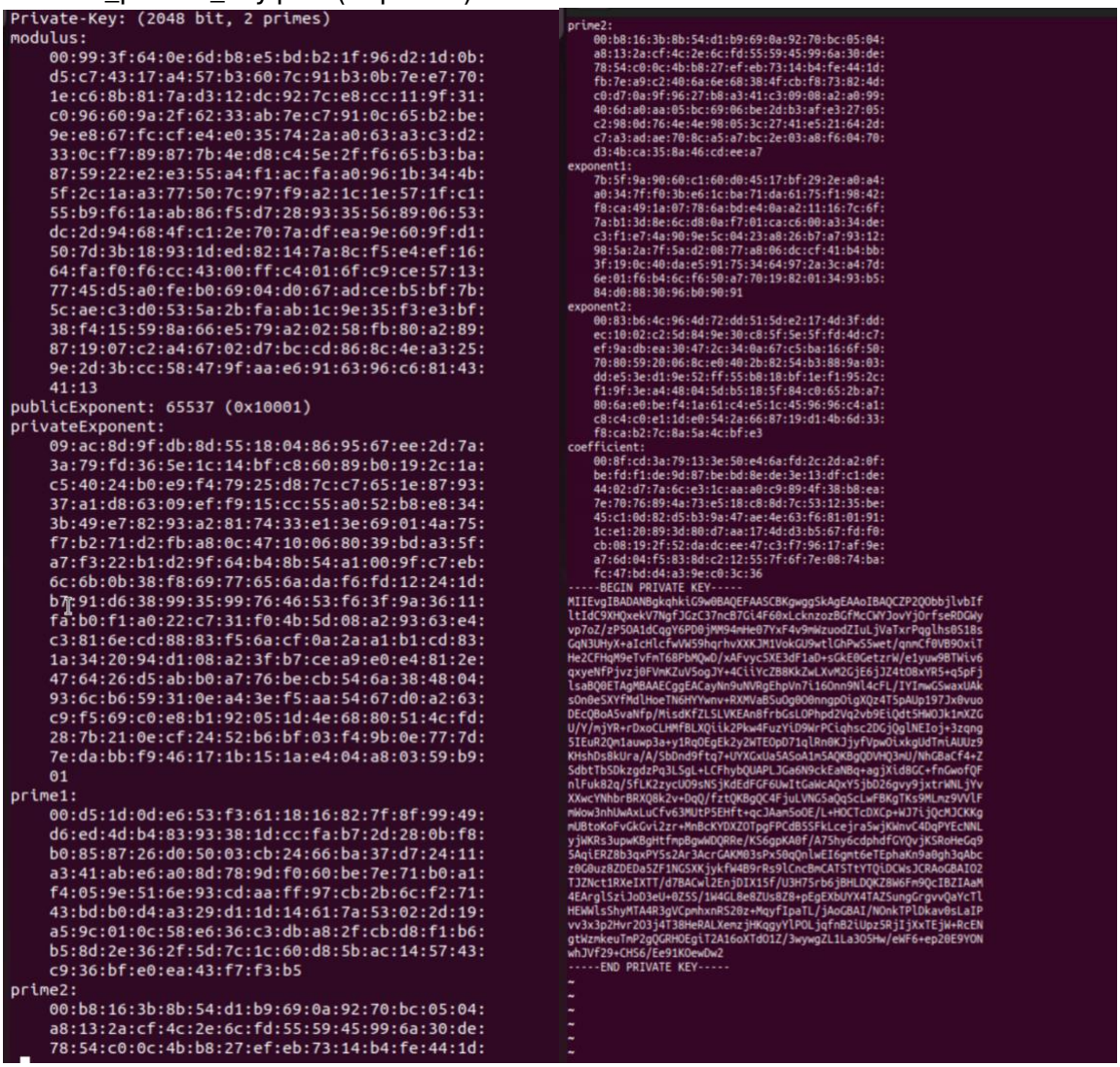
Lab 08 Template – Ethan Roepke

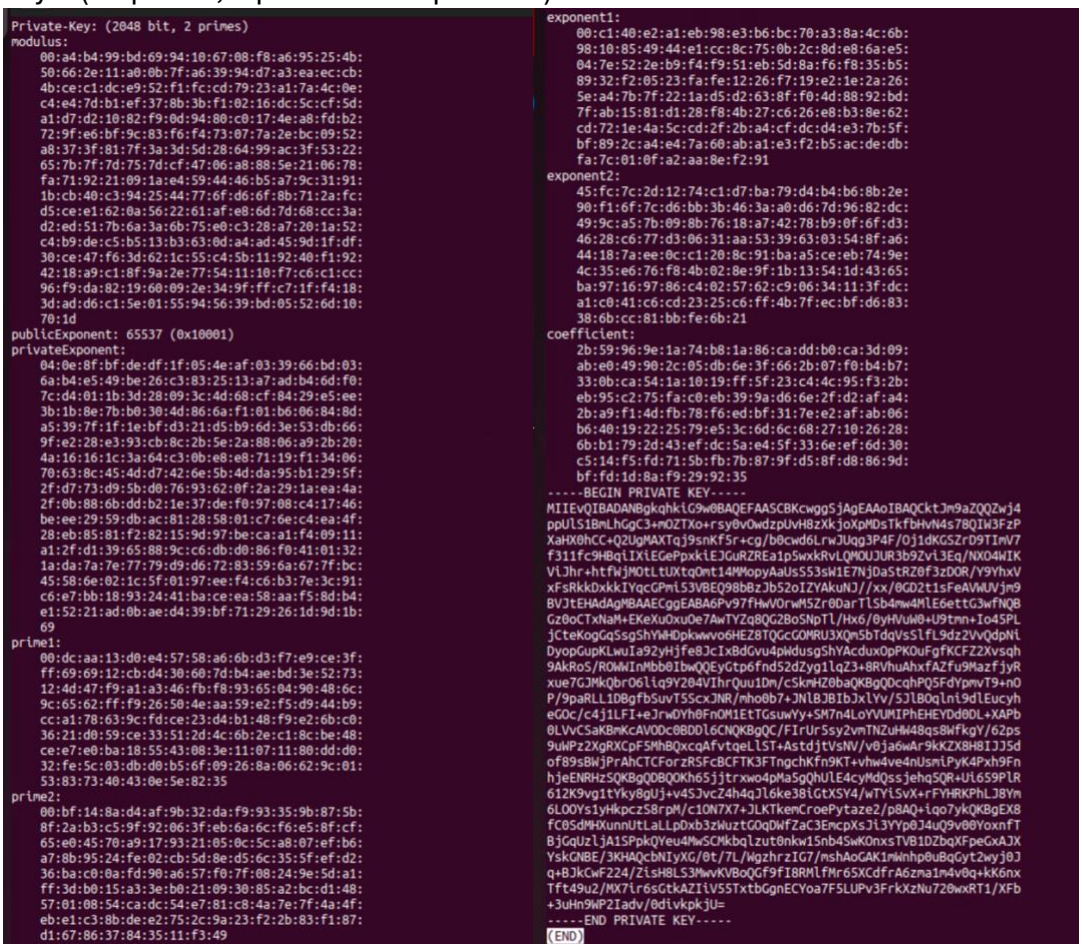
Some questions require multiple parts to be answered, be sure to discuss them in full.

Part 01:

1. **Screenshot of the output from** openssl rsa -text -in <netid>_private_key.pem(10points)



2. **Comparison of the same/different values observed across the extra generated** keys. (15 points, 5 points each question)



   a. Which values are constant?
      The key length bit will stay constant since we are using 2048 bits. The RSA key identifier will stay constant as well
   b. Which ones vary?
      The public key and private key will vary after each new generation. The public key will vary as its mathematically linked to the private key and unique to each pair. The private key will vary because of the random generation for the key.
   c. What do these values represent?
      The public key is distributed to others and allows others to encrypts data with only the matching private key that can decrypt.
      The private key is the secured key that is held with the user and used to decrypt data with public key.
      The key fingerprint is used for quickly verifying kids without revealing the full key data.

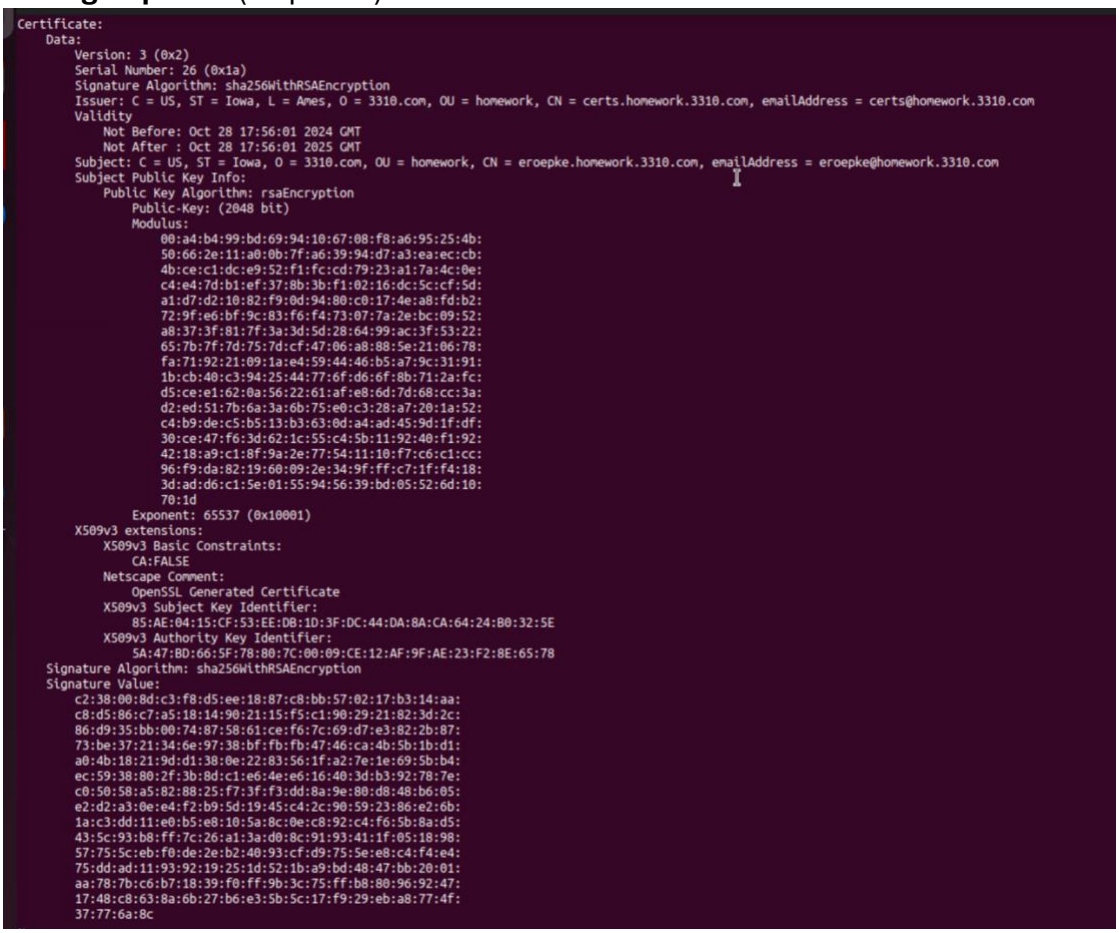
3. **Discussion of the differences between FTP and SFTP.**
   (15 points, 5 points each question)
   a. Why would you want one over the other?
      SFTP offers a secure port for data transfer, while FTP transfers data not secured so in plaintext which is sustainable for attacks. SFTP will encrypt the data and authentication which will protect sensitive data while transferring data. I would want SFTP over FTP for security reasons.
   b. Why did we need to specify our private key?
      We needed to specify our private key to authenticate securely without using just a password. The server will hold the public key and the user would hold the private key and when we specify our private key, only the authorized user with private key can access the server.
   c. What protection does this offer?
      Having public/private key offers much more security not relying on passwords that are prone to brute force. Even an attacker knowing the public key, they cannot get the correct private key since the user has it with them at all times.

4. **Screenshot of the five messages [netid]1.txt, [netid]2.txt, … [netid]5.txt**(10points)

5. **Discussion on hash verification** (10 points, 5 points each question)
   a. What is known about the message?
      From these 5 text messages we gathered, we know that only one of the messages matches the original message that was used to create the signature.
   b. What is the message protected against and what is it vulnerable to?
      The messages are protected against attackers being able to modify the messages from signatures as it will result in a verification failure. The messages is also protected from being able to generate a copy of private key as it can only authenticate the senders identity.
      The messages is vulnerable to MITM attacks if the attacker can get access to the public key and try to trick the sender to verify a forged message

6. **Discussion on what the message generated in step 8e protected against and what it is vulnerable to (compared to the message we downloaded in step 6)** (10 points, 5 points each part)
   The generated message is protected against unauthorized readings so only someone with the matching private key can decrypt it with the public key that decrypts the message. It is also protected against interceptions, so if an attacker does intercept the file during transfer they will not be able to decrypt since they do not have the private key.
   The vulnerabilities from this is not authentication form authority in the server. We are not getting a signature so we cannot confirm the senders identity or if the message was altered. The receiver will not know if anything happened or who it came from since its not verified. Since we have no signature, an attacker can substitute its own public key and trick the sender to encrypt the message with the attacker key and the attacker can decrypt it.
   In step 6, we had authenticity from authorities in the server verifying the messages was not tampered with and the identity is accurate. Step 6 overall provides integrity to who the sender and receiver is.

7. **Screenshot of the signed certificate ([netid]_certificate.pem) when looked at through openssl**(10 points)



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 26 (0x1a)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = Iowa, L = Ames, O = 3310.com, OU = homework, CN = certs.homework.3310.com, emailAddress = certs@homework.3310.com
        Validity
            Not Before: Oct 28 17:56:01 2024 GMT
            Not After : Oct 28 17:56:01 2025 GMT
        Subject: C = US, ST = Iowa, O = 3310.com, OU = homework, CN = eroepke.homework.3310.com, emailAddress = eroepke@homework.3310.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a4:b4:99:bd:69:94:10:67:08:f8:a6:95:25:4b:
                    50:66:2e:11:a0:0b:7f:a6:39:94:d7:a3:ea:ec:cb:
                    4b:ce:c1:dc:e9:52:f1:fc:cd:79:23:a1:7a:4c:0e:
                    c4:e4:7d:b1:ef:37:8b:3b:f1:02:16:dc:5c:cf:5d:
                    a1:d7:d2:10:82:f9:0d:94:80:c0:17:4e:a8:fd:b2:
                    72:9f:e6:bf:9c:83:f6:f4:73:07:7a:2e:bc:09:52:
                    a8:37:3f:81:7f:3a:3d:5d:28:64:99:ac:3f:53:22:
                    65:7b:7f:7d:75:7d:cf:47:06:a8:88:5e:21:06:78:
                    fa:71:92:21:09:1a:e4:59:44:46:b5:a7:9c:31:91:
                    1b:cb:40:c3:94:25:44:77:6f:d6:6f:8b:71:2a:fc:
                    d5:ce:e1:62:0a:56:22:61:af:e8:6d:7d:68:cc:3a:
                    d2:ed:51:7b:6a:3a:6b:75:e0:c3:28:a7:20:1a:52:
                    c4:b9:de:c5:b5:13:b3:63:0d:a4:ad:45:9d:1f:df:
                    30:ce:47:f6:3d:62:1c:55:c4:5b:11:92:40:f1:92:
                    42:18:a9:c1:8f:9a:2e:77:54:11:10:f7:c6:c1:cc:
                    96:f9:da:82:19:60:09:2e:34:9f:ff:c7:1f:f4:18:
                    3d:ad:d6:c1:5e:01:55:94:56:39:bd:05:52:6d:10:
                    70:1d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                85:AE:04:15:CF:53:EE:DB:1D:3F:DC:44:DA:8A:CA:64:24:B0:32:5E
            X509v3 Authority Key Identifier:
                5A:47:BD:66:5F:78:80:7C:00:09:CE:12:AF:9F:AE:23:F2:8E:65:78
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        c2:38:00:8d:c3:f8:d5:ee:18:87:c8:bb:57:02:17:b3:14:aa:
        c8:d5:86:c7:a5:18:14:90:21:15:f5:c1:90:29:21:82:3d:2c:
        86:d9:35:bb:00:74:87:58:61:ce:f6:7c:69:d7:e3:82:2b:87:
        73:be:37:21:34:6e:97:38:bf:fb:fb:47:46:ca:4b:5b:1b:d1:
        a0:4b:18:21:9d:d1:38:0e:22:83:56:1f:a2:7e:1e:69:5b:b4:
        ec:59:38:80:2f:3b:8d:c1:e6:4e:e6:16:40:3d:b3:92:78:7e:
        c0:50:58:a5:82:88:25:f7:3f:f3:dd:8a:9e:80:d8:48:b6:05:
        e2:d2:a3:0e:e4:f2:b9:5d:19:45:c4:2c:90:59:23:86:e2:6b:
        1a:c3:dd:11:e0:b5:e8:10:5a:8c:0e:c8:92:c4:f6:5b:8a:d5:
        43:5c:93:b8:ff:7c:26:a1:3a:d0:8c:91:93:41:1f:05:18:98:
        57:75:5c:eb:f0:de:2e:b2:40:93:cf:d9:75:5e:e8:c4:f4:e4:
        75:dd:ad:11:93:92:19:25:1d:52:1b:a9:bd:48:47:bb:20:01:
        aa:78:7b:c6:b7:18:39:f0:ff:9b:3c:75:ff:b8:80:96:92:47:
        17:48:c8:63:8a:6b:27:b6:e3:5b:5c:17:f9:29:eb:a8:77:4f:
        37:77:6a:8c
```

8. **Discussion from step 12** (20 points, 10 points each answer, 10 points each why)
    a. Do any parts of the certificate match with your private key? If so, why?
    None of the certificate match with my private key because the certificate only contains parts from the public key. The private key is securely stored with me and not appear in anything.
    b. What was happening during the Certificate Signing process? Why did you need to submit it for signing?
    During the certificate signing process, my public key and questions I was prompted to answer was submitted to an authority on server. The authority verifies your identity which create a certificate to prove your identity. The authority also guarantees that the information has not been tampered between public and private key.
    We need to submit it for signing by authority to establish trust and security. A signed certificate verifies that the public key belongs to the organization and not a forgery.